IL WEB È DIVENTATO UN LUOGO PERICOLOSO? POSSIAMO DIFENDERCI!

Data: Venerdì 12 maggio (8 ore)
Sede: *Federmanager Bologna -Ravenna – Via Bombicci 1 – Bologna*
Orario: *dalle 9.00 – 18.00*
Per informazioni e iscrizioni : Sara Tirelli - Federmanager Bologna – Ravenna
tel. 051 0366618
sara.tirelli@federmanagerbo.it

In questo corso verranno trattati i temi di Sicurezza Informatica, con particolare attenzione agli attacchi del Cybercrime ed alla protezione dei propri dati e dei propri account. Spiegheremo perché oggi la Cyber Security riguarda tutti noi e perché nessuno può considerarsi al sicuro: ritenere di non essere un obbiettivo interessante per i cyber criminali è il miglior presupposto per essere attaccati. Gli strumenti informatici sono importanti, ma il punto debole è sempre l'uomo (il fattore "H") che con il suo comportamento può rendere inefficace qualsiasi strumento di difesa. L'uso di password deboli è una delle principali cause (63%) della violazione e del furto dei nostri dati: cosa fare per proteggerci meglio?
Non serve essere dei "geni" dell'informatica per riuscire a difendersi: basta acquisire la consapevolezza dei rischi e saperli riconoscere. In una parola: "usare la testa".

CONTENUTI

L'evoluzione del Cybercrime

- I dati del crimine informatico nell'Italia e nel mondo: il rapporto CLUSIT 2017.
- Cyberwarfare, la guerra cibernetica: casi famosi.
- Il Deep Web ed il Dark Web: cosa sono e perché non sono la stessa cosa.
- I danni economici generati alle aziende.
- I problemi ed i rischi nelle PMI e negli studi professionali.
- Nelle aziende il pericolo arriva soprattutto dall'interno.

Gli attacchi che dobbiamo temere di più: come difendersi

- Gli attacchi attraverso la posta elettronica.
- La crittografia dell'email: PGP (Pretty Good Privacy).
- Messaggistica istantanea: WhatsApp, Telegram, Messenger. Ci possiamo fidare?
- Il CryptoLocker non è un malware, è un disastro: storia e diffusione.
- I Ransomware: come ci attaccano e come proteggersi.
- Cos'è il Social Engineering e come difendersi.
- La vulnerabilità dei siti web: i rischi di WordPress e dei CMS open source.
- I Malware su devices mobili (sempre più diffusi).
- Le reti WI-FI: i problemi di sicurezza delle reti aperte.

Imparare ad usare le Password

- Gli strumenti (sempre più potenti) degli hackers: alcuni famosi casi di attacchi e "data breach".
- La sicurezza di un Account dipende dalla forza della password.
- Le regole per una Password sicura e gli errori da evitare.
- Le "domande di sicurezza".
- I Password Manager.
- L'autenticazione a due fattori (MFA: Multi factor authentication)

Mettere in pratica la Cyber Security

- Che cos'è la ISO/IEC 27001.
- Il tramonto degli Antivirus: ormai non ci proteggono più.
- I sistemi di protezione avanzata più efficaci: User Behavior Analytics (UBA).
- L'importanza del Backup: 3-2-1 Backup Strategy.
- La Sicurezza Informatica come "Gioco di squadra".

OBIETTIVI

- Fornire strumenti e strategie per la sicurezza informatica in azienda e nella pratica di ogni giorno
- Imparare a riconoscere i ransomware e malware più comuni oggi sul web e ad evitarli
- Imparare a scegliere ed usare le password per proteggere i dati

DOCENTE: Giorgio Sbaraglia. Ingegnere, ha ricoperto per molti anni la funzione di Direttore Acquisti presso una grande società di costruzioni e, precedentemente, presso aziende metalmeccaniche e manifatturiere del territorio. Appassionato e conoscitore dei temi di sicurezza informatica in azienda, svolge attività di consulenza aziendale ed in collaborazione con diverse società di formazione, tiene corsi di formazione in materia di Cyber Security.
È membro del CLUSIT (Associazione Italiana per la Sicurezza Informatica).

www.giorgiosbaraglia.it